(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－69175
（P2001－69175A）
(43)公開日　平成13年３月16日(2001.3.16)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　11/20	Ｂ	５Ｂ０８９
Ｇ０６Ｆ　13/00	３５３	Ｇ０６Ｆ　13/00	３５３Ｃ	５Ｋ０３０
Ｈ０４Ｌ　12/56		Ｈ０４Ｌ　11/20	１０２Ｚ	

審査請求　未請求　請求項の数11　ＯＬ　（全 15 頁）

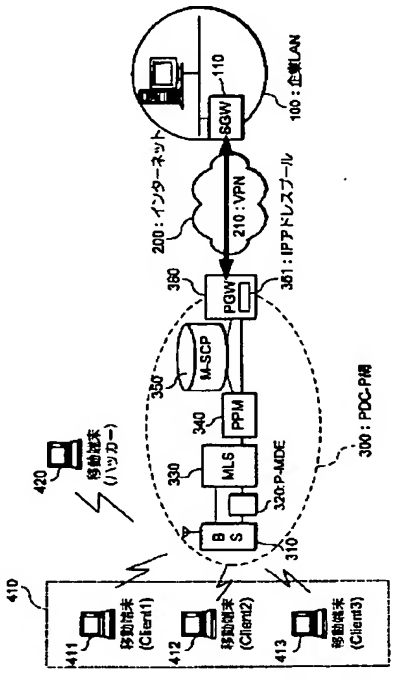
(21)出願番号　特願平11－242013
(22)出願日　平成11年８月27日(1999.8.27)

(71)出願人　392026693
株式会社エヌ・ティ・ティ・ドコモ
東京都千代田区永田町二丁目11番１号
(72)発明者　高橋　竜男
東京都港区虎ノ門二丁目10番１号　エヌ・ティ・ティ移動通信網株式会社内
(72)発明者　竹下　敦
東京都港区虎ノ門二丁目10番１号　エヌ・ティ・ティ移動通信網株式会社内
(74)代理人　100098084
弁理士　川▲崎▼　研二　（外２名）

最終頁に続く

(54)【発明の名称】　セッション情報管理方法およびセッション情報管理装置

(57)【要約】
【課題】　クライアントとサーバとを接続する仮想私設網において、安定的な通信を確保しながら低コストでセッション情報の資源枯渇を防止する。
【解決手段】　セキュリティゲートウェイ１１０は、総セッション数制限の範囲をこえた時点で「死んでいる」可能性の高い削除候補セッションを選択し、順次セッションが生きているか否かの状況確認を行い、「死んでいる」セッションと確認できたセッションを削除していくので、削除ミスの可能性を極めて小さくすることができる。また、キープアライブパケットを使用しなくても「死んでいる」セッションを削除できるので、キープアライブパケットに対する課金がなくなり、移動端末４００のユーザは通信コストを削減することができる。



1

【特許請求の範囲】

【請求項１】　クライアントとサーバとを接続する仮想私設網におけるセッション情報管理方法であって、

クライアントの認証情報およびアドレス情報を含んだセッション設定要求をうけるセッション設定要求段階と、

前記セッション設定要求が所定の条件を満たす場合には、当該セッション設定要求に基づいてセッション情報を生成して記憶するセッション情報記憶段階と、

前記セッション設定要求に基づいて生成されるべきセッション情報が前記サーバ側において設定可能な総セッション数をこえた場合には、記憶されている前記セッション情報から削除すべき候補を所定の規則に従って選択する削除候補選択段階と、

前記選択された削除候補のセッション情報として記憶された前記クライアントのアドレスに対して前記仮想私設網における接続状況の確認を行う接続状況確認段階と、

前記接続状況の確認に対して接続状況が正常である旨の応答が得られない場合には、当該状況確認に対応する前記セッション情報を削除するセッション情報削除段階とを備えることを特徴とするセッション情報管理方法。

【請求項２】　請求項１に記載のセッション情報管理方法において、

前記所定の規則に従って選択される優先順位は、生成されてからの経過時間が長い前記セッション情報である程高いことを特徴とするセッション情報管理方法。

【請求項３】　請求項１に記載のセッション情報管理方法において、

前記所定の規則に従って選択される優先順位は、最後に使用されてからの経過時間が長い前記セッション情報である程高いことを特徴とするセッション情報管理方法。

【請求項４】　請求項１に記載のセッション情報管理方法において、

クライアントから前記接続状況の確認に対して接続状況が正常である旨の応答が得られた場合には、当該状況確認に対応する前記セッション情報について、前記所定の規則に従って選択される優先順位を低く設定する優先順位設定段階を備えることを特徴とするセッション情報管理方法。

【請求項５】　クライアントとサーバとを接続する仮想私設網におけるセッション情報管理方法であって、

クライアントの認証情報およびアドレス情報を含んだセッション設定要求をうけるセッション設定要求段階と、

前記セッション設定要求が所定の条件を満たす場合には、当該セッション設定要求に基づいてセッション情報を生成して記憶するセッション情報記憶段階と、

前記セッション設定要求に基づいて生成されるべきセッション情報が前記サーバ側において同時に接続可能なセッション数をこえた場合には、当該セッション設定要求に含まれたクライアントを特定する情報に対応する前記記憶したセッション情報を選択する選択段階と、

2

前記選択されたセッション情報として記憶された前記クライアントのアドレスに対して前記仮想私設網における接続状況の確認を行う接続状況確認段階と、

前記接続状況の確認に対して接続状況が正常である旨の応答が得られない場合には、当該状況確認に対応する前記セッション情報を削除するセッション情報削除段階とを備えることを特徴とするセッション情報管理方法。

【請求項６】　クライアントとサーバとを接続する仮想私設網におけるセッション情報管理方法であって、

クライアントの認証情報およびアドレス情報を含んだセッション設定要求をうけるセッション設定要求段階と、

前記セッション設定要求が所定の条件を満たす場合には、当該セッション設定要求に基づいてセッション情報を生成して記憶するセッション情報記憶段階と、

前記セッション設定要求に基づいて生成されるべきセッション情報が前記サーバ側において同時に接続可能なセッション数をこえた場合には、当該セッション設定要求に含まれたクライアントを特定する情報に対応する前記記憶したセッション情報を選択する選択段階と、

前記選択されたセッション情報として記憶された前記クライアントのアドレスに対して前記仮想私設網における接続状況の確認を行う接続状況確認段階と、

クライアントから前記接続状況の確認に対して接続状況が正常である旨の応答が得られた場合には、前記前記セッション設定要求を拒絶する拒絶段階とを備えることを特徴とするセッション情報管理方法。

【請求項７】　請求項６に記載のセッション情報管理方法において、

前記セッション設定要求を拒絶する場合には、当該セッション設定要求に含まれる前記認証情報およびアドレス情報をアクセス拒否情報として記憶する拒否情報記憶段階を備えることを特徴とするセッション情報管理方法。

【請求項８】　請求項７に記載のセッション情報管理方法において、

前記セッション設定要求が前記アクセス拒否情報として記憶された認証情報およびアドレス情報と一致する場合には前記前記セッション設定要求を拒絶する第２の拒絶段階を備えることを特徴とするセッション情報管理方法。

【請求項９】　クライアントとサーバとを接続する仮想私設網におけるセッション情報管理を行うセッション情報管理装置であって、

クライアントの認証情報およびアドレス情報を含んだセッション設定要求が所定の条件を満たす場合には、クライアントの認証情報およびアドレス情報とを対応つけてセッション情報として記憶するセッション情報記憶手段と、

前記セッション設定要求に基づいて生成されるべきセッション情報が前記サーバ側において設定可能な総セッション数をこえた場合には、記憶されている前記セッショ

ン情報から削除すべき候補を所定の規則に従って選択する削除候補選択手段と、
前記選択された削除候補のセッション情報として記憶された前記クライアントのアドレスに対して前記仮想私設網における接続状況の確認を行う接続状況確認手段と、
前記接続状況の確認に対して接続状況が正常である旨の応答が得られない場合には、当該状況確認に対応する前記セッション情報を削除するセッション情報削除手段とを備えることを特徴とするセッション情報管理装置。
【請求項１０】　クライアントとサーバとを接続する仮想私設網におけるセッション情報管理を行うセッション情報管理装置であって、
クライアントの認証情報およびアドレス情報を含んだセッション設定要求が所定の条件を満たす場合には、当該セッション設定要求に基づいてセッション情報を生成して記憶するセッション情報記憶手段と、
前記セッション設定要求に基づいて生成されるべきセッション情報が前記サーバ側において同時に接続可能なセッション数をこえた場合には、当該セッション設定要求に含まれたクライアントを特定する情報に対応する前記記憶したセッション情報を選択する選択手段と、
前記選択されたセッション情報として記憶された前記クライアントのアドレスに対して前記仮想私設網における接続状況の確認を行う接続状況確認手段と、
前記接続状況の確認に対して接続状況が正常である旨の応答が得られない場合には、当該状況確認に対応する前記セッション情報を削除するセッション情報削除手段とを備えることを特徴とするセッション情報管理装置。
【請求項１１】　クライアントとサーバとを接続する仮想私設網におけるセッション情報管理を行うセッション情報管理装置であって、
クライアントの認証情報およびアドレス情報を含んだセッション設定要求が所定の条件を満たす場合には、当該セッション設定要求に基づいてセッション情報を生成して記憶するセッション情報記憶手段と、
前記セッション設定要求に基づいて生成されるべきセッション情報が前記サーバ側において同時に接続可能なセッション数をこえた場合には、当該セッション設定要求に含まれたクライアントを特定する情報に対応する前記記憶したセッション情報を選択する選択手段と、
前記選択されたセッション情報として記憶されたに前記クライアントのアドレスに対して前記仮想私設網における接続状況の確認を行う接続状況確認手段と、
クライアントから前記接続状況の確認に対して接続状況が正常である旨の応答が得られた場合には、前記前記セッション設定要求を拒絶する拒絶手段とを備えることを特徴とするセッション情報管理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、クライアントとサーバとを接続する仮想私設網におけるセッション情報管理を行うセッション情報管理方法およびセッション情報管理装置に関する。
【０００２】
【従来の技術】従来より、通信端末装置（クライアント）が電話網を介して最寄りのインターネット接続点に接続（いわゆるダイアルアップ接続）し、さらに、インターネットを介してサーバ側のネットワーク（例えば企業ＬＡＮ（Local Area Network））に接続する場合において、インターネット上を安全に通過するために仮想私設網（Virtual Private Network：ＶＰＮ）を構築するいわゆるダイアルアップＶＰＮが知られている。仮想私設網とは、暗号技術や、認証技術、トンネリング技術などを利用して、インターネット上においても専用線と同様の安全性および利便性を有する通信を実現する技術である。このような仮想私設網機能を実現するネットワークコンポーネントをセキュリティゲートウェイ（Security GateWay：ＳＧＷ）という。
【０００３】仮想私設網においては、通常はＩＰ（Internet Protocol）アドレスを用いて通信相手を識別する。ところで、ＩＰアドレスは、クライアント毎に固定されている場合もあるが、クライアントがダイヤルアップ接続を行っている場合には、接続を行う度に異なっている場合がある。具体的には、ダイヤルアップクライアントに割り当てるためのＩＰアドレスを一定数確保しているインターネット接続点に電話網を介して接続要求を行うことによって、ダイヤルアップクライアントは利用可能なＩＰアドレスが適宜割り当てられるようになっている。従って、ダイアルアップＶＰＮにおいては、仮想私設網を終端するクライアントがダイアルアップ接続を行っている場合には、仮想私設網の他端となるセキュリティゲートウェイはＩＰアドレスからクライアントを識別することができないことになる。
【０００４】そこで、セキュリティゲートウェイはＩＰよりも上位層のプロトコルでクライアントの認証を行う必要があり、一般的にはユーザＩＤおよびパスワードを組み合わせた情報や、デジタル署名などの情報を用いて認証を行っている。このような認証を行った後、クライアントおよびセキュリティゲートウェイ間の通信を行うために、ＩＰアドレス等の情報や仮想私設網におけるセキュリティポリシなどのネゴシエーションを行う。クライアントおよびセキュリティゲートウェイは、ネゴシエーションにおける情報を双方でセッション情報として保存する。このようにしてクライアントがセキュリティゲートウェイに接続することによって、企業ＬＡＮ内にいるのと同様の環境で、企業内各種サーバに接続し、所望のサービスを利用することが可能となっている。
【０００５】
【発明が解決しようとする課題】このような仮想私設網のセッション設定から解放までは、

（１）クライアントからインターネット接続点へ接続
（２）クライアント・セキュリティゲートウェイ間にセッション設定
（３）クライアント・サーバ間通信
（４）クライアント・サーバ間セッション断
（６）クライアント・セキュリティゲートウェイ間セッション断
（７）クライアントからインターネット接続点へのコネクション断
という手順が踏まれるのが通常である。しかしながら、クライアント・インターネット接続点間の接続が切断されてしまい、クライアントが正常な手順を踏まない状態で終了してしまう場合も生じることがある。例えば、クライアントの電源が遮断されてしまった場合や、インターネット接続点の故障、無線網を介してインターネット接続点に接続しているクライアントが圏外に移動してしまった場合などが考えられる。なお、以下の説明において、クライアント・インターネット接続点間が接続されている状態を「生きているセッション」といい、クライアント・インターネット接続点間の接続が切断されている状態を「死んだセッション」というものとする。

【０００６】このように、正常な手順を踏まずに終了すると、セッションに関して以下のような問題が生じる。クライアントは電話網を介してインターネットに接続しているので、クライアント・インターネット接続点間の接続状態（セッションの生死）を直ちに検出することができるが、これに対してセキュリティゲートウェイはインターネットに接続しているのでクライアント・インターネット接続点間の接続状態を直接検出することはできない。サーバからクライアントへパケットを送信するシーケンスの途中にクライアント・インターネット接続点間の接続が切断された場合は、パケットはクライアントへ到達しないので、セキュリティゲートウェイはクライアント・インターネット接続点間の接続が切断された状態をパケットの不達によって間接的に検出する。

【０００７】しかしながら、パケットの不達を検出できないような場合、例えば、サーバがクライアントから要求待ちであるような場合や、クライアント・サーバ間のセッションが確立していないような場合、あるいは、セッションが確立していても使用されていない場合には、セキュリティゲートウェイはクライアント・インターネット接続点間の接続が切断された状態を直接的にも間接的にも検出することができない。このようにセキュリティゲートウェイがクライアント・インターネット接続点間の接続を検出できないために、「死んだセッション」をセキュリティゲートウェイが保存したままになると、セキュリティゲートウェイではセッション資源が枯渇しまうという問題が生じる。あるいは、電話網側の回線状況などが原因で、インターネット接続点への接続が切断されたクライアントが再度インターネット接続点に

接続した場合は、以前に使用していたものとは異なるＩＰアドレスが割り当てられるので、クライアントがセキュリティゲートウェイに仮想私設網セッション設定を再要求した場合には、以前のセッション情報が保存されているために新しいセッションの設定を拒絶してしまうという問題も生じる。セキュリティゲートウェイでは、同一ユーザＩＤのクライアントが同時に複数のセッションを設定することはセキュリティ上の理由で制限しているからである。このような問題を解決するためには、一定時間利用されないセッションをセキュリティゲートウェイが自動的に削除するように設定することも可能であるが、このような場合はクライアント側が長時間通信を行わない場合にはセッションを削除されてしまうという不都合があり、クライアントには不便になっていまう。

【０００８】そこで、従来は一定周期毎にサーバからクライアントに状態確認のパケット（キープアライブパケット）を送り、クライアントはキープアライブパケットを受け取るとただちに正常である旨の応答を行うようにして、サーバは規定時間以内に応答が帰ってこなかった場合にクライアントがセッションを停止したと判断してセッション情報を削除する、という対応がなされていた。しかしながら、クライアントが接続している電話網が、送受信データ量に対して課金される、いわゆるパケット交換方式の電話網である場合、このようなキープアライブパケットを用いると、一定周期毎にパケットの交換が行われ、個々のキープアライブパケットに対して課金が行われてしまうので、クライアント側ユーザの通信コストがかさんでしまうという問題があった。あるいは、電話網やインターネットの一時的な輻輳などによりパケットの伝達遅延が生じてしまった場合には、キープアライブパケットに対する応答が規定時間内に戻らないので、セッションは生きているにもかかわらずセッション情報が削除されてしまい、安定した通信を行うことができないという問題もあった。このように、従来のセッション管理方法においては、安定的な通信を確保しながら低コストでセッション情報の資源枯渇を防止することは困難であった。

【０００９】本発明は、上述した課題を解決するためになされたものであり、安定的な通信を確保しながら低コストでセッション情報の資源枯渇を防止することができるセッション情報管理方法およびセッション情報管理装置を提供することを目的としている。

【００１０】

【課題を解決するための手段】上述した課題を解決するために、請求項１に記載の発明は、クライアントとサーバとを接続する仮想私設網におけるセッション情報管理方法であって、クライアントの認証情報およびアドレス情報を含んだセッション設定要求をうけるセッション設定要求段階と、前記セッション設定要求が所定の条件を満たす場合には、当該セッション設定要求に基づいてセ

ッション情報を生成して記憶するセッション情報記憶段階と、前記セッション設定要求に基づいて生成されるべきセッション情報が前記サーバ側において設定可能な総セッション数をこえた場合には、記憶されている前記セッション情報から削除すべき候補を所定の規則に従って選択する削除候補選択段階と、前記選択された削除候補のセッション情報として記憶された前記クライアントのアドレスに対して前記仮想私設網における接続状況の確認を行う接続状況確認段階と、前記接続状況の確認に対して接続状況が正常である旨の応答が得られない場合には、当該状況確認に対応する前記セッション情報を削除するセッション情報削除段階とを備えることを特徴とする。

【００１１】請求項２に記載の発明は、請求項１に記載のセッション情報管理方法において、前記所定の規則に従って選択される優先順位は、生成されてからの経過時間が長い前記セッション情報である程高いことを特徴とする。請求項３に記載の発明は、請求項１に記載のセッション情報管理方法において、前記所定の規則に従って選択される優先順位は、最後に使用されてからの経過時間が長い前記セッション情報である程高いことを特徴とする。請求項４に記載の発明は、請求項１に記載のセッション情報管理方法において、クライアントから前記接続状況の確認に対して接続状況が正常である旨の応答が得られた場合には、当該状況確認に対応する前記セッション情報について、前記所定の規則に従って選択される優先順位を低く設定する優先順位設定段階を備えることを特徴とする。

【００１２】請求項５に記載の発明は、クライアントとサーバとを接続する仮想私設網におけるセッション情報管理方法であって、クライアントの認証情報およびアドレス情報を含んだセッション設定要求をうけるセッション設定要求段階と、前記セッション設定要求が所定の条件を満たす場合には、当該セッション設定要求に基づいてセッション情報を生成して記憶するセッション情報記憶段階と、前記セッション設定要求に基づいて生成されるべきセッション情報が前記サーバ側において同時に接続可能なセッション数をこえた場合には、当該セッション設定要求に含まれたクライアントを特定する情報に対応する前記記憶したセッション情報を選択する選択段階と、前記選択されたセッション情報として記憶された前記クライアントのアドレスに対して前記仮想私設網における接続状況の確認を行う接続状況確認段階と、前記接続状況の確認に対して接続状況が正常である旨の応答が得られない場合には、当該状況確認に対応する前記セッション情報を削除するセッション情報削除段階とを備えることを特徴とする。

【００１３】請求項６に記載の発明は、クライアントとサーバとを接続する仮想私設網におけるセッション情報管理方法であって、クライアントの認証情報およびアドレス情報を含んだセッション設定要求をうけるセッション設定要求段階と、前記セッション設定要求が所定の条件を満たす場合には、当該セッション設定要求に基づいてセッション情報を生成して記憶するセッション情報記憶段階と、前記セッション設定要求に基づいて生成されるべきセッション情報が前記サーバ側において同時に接続可能なセッション数をこえた場合には、当該セッション設定要求に含まれたクライアントを特定する情報に対応する前記記憶したセッション情報を選択する選択段階と、前記選択されたセッション情報として記憶された前記クライアントのアドレスに対して前記仮想私設網における接続状況の確認を行う接続状況確認段階と、クライアントから前記接続状況の確認に対して接続状況が正常である旨の応答が得られた場合には、前記前記セッション設定要求を拒絶する拒絶段階とを備えることを特徴とする。請求項７に記載の発明は、請求項６に記載のセッション情報管理方法において、前記セッション設定要求を拒絶する場合には、当該セッション設定要求に含まれる前記認証情報およびアドレス情報をアクセス拒否情報として記憶する拒否情報記憶段階を備えることを特徴とする。請求項８に記載の発明は、請求項７に記載のセッション情報管理方法において、前記セッション設定要求が前記アクセス拒否情報として記憶された認証情報およびアドレス情報と一致する場合には前記前記セッション設定要求を拒絶する第２の拒絶段階を備えることを特徴とする。

【００１４】請求項９に記載の発明は、クライアントとサーバとを接続する仮想私設網におけるセッション情報管理を行うセッション情報管理装置であって、クライアントの認証情報およびアドレス情報を含んだセッション設定要求が所定の条件を満たす場合には、クライアントの認証情報およびアドレス情報とを対応つけてセッション情報として記憶するセッション情報記憶手段と、前記セッション設定要求に基づいて生成されるべきセッション情報が前記サーバ側において設定可能な総セッション数をこえた場合には、記憶されている前記セッション情報から削除すべき候補を所定の規則に従って選択する削除候補選択手段と、前記選択された削除候補のセッション情報として記憶された前記クライアントのアドレスに対して前記仮想私設網における接続状況の確認を行う接続状況確認手段と、前記接続状況の確認に対して接続状況が正常である旨の応答が得られない場合には、当該状況確認に対応する前記セッション情報を削除するセッション情報削除手段とを備えることを特徴とする。

【００１５】請求項１０に記載の発明は、クライアントとサーバとを接続する仮想私設網におけるセッション情報管理を行うセッション情報管理装置であって、クライアントの認証情報およびアドレス情報を含んだセッション設定要求が所定の条件を満たす場合には、当該セッション設定要求に基づいてセッション情報を生成して記憶

するセッション情報記憶手段と、前記セッション設定要求に基づいて生成されるべきセッション情報が前記サーバ側において同時に接続可能なセッション数をこえた場合には、当該セッション設定要求に含まれたクライアントを特定する情報に対応する前記記憶したセッション情報を選択する選択手段と、前記選択されたセッション情報として記憶された前記クライアントのアドレスに対して前記仮想私設網における接続状況の確認を行う接続状況確認手段と、前記接続状況の確認に対して接続状況が正常である旨の応答が得られない場合には、当該状況確認に対応する前記セッション情報を削除するセッション情報削除手段とを備えることを特徴とする。

【００１６】請求項１１に記載の発明は、クライアントとサーバとを接続する仮想私設網におけるセッション情報管理を行うセッション情報管理装置であって、クライアントの認証情報およびアドレス情報を含んだセッション設定要求が所定の条件を満たす場合には、当該セッション設定要求に基づいてセッション情報を生成して記憶するセッション情報記憶手段と、前記セッション設定要求に基づいて生成されるべきセッション情報が前記サーバ側において同時に接続可能なセッション数をこえた場合には、当該セッション設定要求に含まれたクライアントを特定する情報に対応する前記記憶したセッション情報を選択する選択手段と、前記選択されたセッション情報として記憶されたに前記クライアントのアドレスに対して前記仮想私設網における接続状況の確認を行う接続状況確認手段と、クライアントから前記接続状況の確認に対して接続状況が正常である旨の応答が得られた場合には、前記前記セッション設定要求を拒絶する拒絶手段とを備えることを特徴とする。

【００１７】

【発明の実施の形態】以下、図面を参照しながら本発明の実施の形態について説明する。

【００１８】［１．実施形態の構成］

［１－１．全体構成］図１は実施形態の全体構成を示す図である。図１に示すように、本実施形態では、企業ＬＡＮ１００に対して、セキュリティゲートウェイ１１０を終端としてインターネット２００に設定された仮想私設網２１０および移動通信網３００を介して移動端末４１１、４１２、４１３、４２０（特定を要さない場合は移動端末４００と記す）が接続できるようにようになっている。

【００１９】本実施形態では、移動通信網３００にはＰＤＣ移動パケット通信システム（Personal Digital Cellular－Packet：ＰＤＣ－Ｐ）を用いており、移動通信網３００は、基地局（Base Station：ＢＳ）３１０、パケット用基地局変復調装置（Packet Modulation/Demodulation Equipment：Ｐ－ＭＤＥ）３２０、加入者交換機（Mobile Local Switch：ＭＬＳ）３３０、パケット加入者系処理装置（Packet Processing Module：ＰＰＭ）３４０、移動通信サービス制御装置（Mobile Service Control－Point：Ｍ－ＳＣＰ）３５０、パケットゲートウェイ（PacketGateWay：ＰＧＷ）３６０を備えて構成されている。基地局３１０は、パケット通信機能を有するパケット用基地局変復調装置３２０に接続されており、移動端末４００への高速なパケットエアインターフェイスを提供する。パケット加入者系処理装置３４０は、基地局３１０を介して移動端末４００と対向し、パケットを送受信するものであり、無線区間のパケットの組立・分解、認証、秘匿、課金などを行う。本実施形態では、企業ＬＡＮ１００から移動端末４００への下りパケットに対する課金ポイントとして機能し、移動端末４００から下りパケットに対する応答を示すＡＣＫ（Acknowledge）を受信した時点で課金を行う。移動通信サービス制御装置３５０は、移動端末４００の存在するエリアや加入者のサービス情報を記憶する網内データベースを備え、パケットゲートウェイ３６０は、インターネット２００など他網から移動端末４００へのパケット着信時に移動通信サービス制御装置３５０が有する位置情報へアクセスして、移動端末４００の存在するエリアを管理しているパケット加入者系処理装置３４０へルーチングする。

【００２０】パケットゲートウェイ３６０は、インターネット接続点としての機能とともに、移動端末４００から企業ＬＡＮ１００への上りパケットへの課金ポイントとしての機能を有している。パケットゲートウェイ３６０は、ＩＰアドレスプール３６１を備えており、移動端末４００から接続要求があった時点で利用可能なＩＰアドレスの中から任意の一つを選択的に割り当てる。移動端末４００は、仮想私設網２１０を介して企業ＬＡＮ１００へ接続する場合にはインターネット接続点であるパケットゲートウェイ３６０へ接続を行い、接続を行う度に異なるＩＰアドレスの割り当てを受けることによって、企業ＬＡＮ１００へパケットを送信することができるようになる。パケットゲートウェイ３６０は、インターフェイス２００にパケットが送信された時点で課金を行う。

【００２１】本実施形態においては、移動端末４１１、４１２、４１３（特定を要さない場合は移動端末４１０と記す）は、企業ＬＡＮ１００に対する正当な権限を有するユーザが使用する通信端末装置であり、移動端末４２０は、企業ＬＡＮ１００に対して正当なアクセス権限を有さない者（いわゆるハッカー）が使用する通信端末装置である。正当権限を有する移動端末４１０それぞれのユーザには企業ＬＡＮ１００における固有のユーザＩＤが割り当てられている。本実施形態では、移動端末４１１のユーザには“Client1”というユーザＩＤが割り当てられ、移動端末４１２のユーザには“Client2”というユーザＩＤが割り当てられ、移動端末４１３のユーザには“Client3”というユーザＩＤが割り当てられて

おり、これらのユーザＩＤは、後に詳しく説明するように、企業ＬＡＮ１００内において各移動端末４１０のユーザを識別する情報として管理されている。なお、移動端末４２０のユーザであるハッカーにはユーザＩＤは割り当てられておらず、正当権限者からユーザＩＤおよびパスワードなどの認証情報を不正に入手して企業ＬＡＮ１００に対して接続を試みる。本実施形態では、ユーザＩＤ、パスワード、ＩＰアドレスなどの情報を用いて、企業ＬＡＮ１００と移動端末４００とのセッションが設定されると、後に詳しく説明するようにセキュリティゲートウェイ１１０および移動端末４００はセッション情報をそれぞれ保存して、仮想私設網２１０上における通信を安定的に行うとともに第三者の不正なアクセスを防止するようになっている。

【００２２】［１－２．セキュリティゲートウェイの構成］次に、セキュリティゲートウェイ１１０についてより詳細に説明する。図２は、セキュリティゲートウェイ１１０の機能構成を示すブロック図である。セキュリティゲートウェイ１１０は、インターネット２００とインターフェイスであるインターネット接続部１１１、認証を制御する認証制御部１１２、ユーザＩＤやパスワードなどのユーザ認証情報を記憶するユーザ情報記憶部１１３、不正なアクセスを拒否するための情報を記憶するアクセス拒否情報記憶部１１４、セッションに関する各種制御を行うセッション制御部１１５、セッション情報を記憶するセッション記憶部１１６、および、企業ＬＡＮ１００内のインターフェイスであるＬＡＮ接続部１１７を備えている。

【００２３】ここで、図３を参照しながら、セッション情報１１６、ユーザ情報記憶部１１３、およびアクセス拒否情報記憶部１１４に記憶される情報について説明しておく。セッション情報記憶部１１６には、それぞれ異なるセッション番号毎にクライアントのＩＰアドレスおよびユーザＩＤを対応付けたセッション情報が記憶されている。セッション番号が付される規則については、後に説明する。ユーザ情報記憶部１１３には、企業ＬＡＮ１００へのアクセス権限を有する各ユーザに割り当てられたユーザＩＤ毎に各ユーザが設定したパスワードを対応つけたユーザ情報が記憶されている。また、アクセス拒否情報記憶部１１４には、不正なアクセスと判定されたユーザＩＤ毎に、不正なアクセスを行った際に用いられたＩＰアドレスが対応つけられたアクセス拒否情報が記憶されている。アクセス拒否情報が示すユーザＩＤは、ハッカーが正当なユーザから不正に入手したユーザＩＤであって、ユーザＩＤ自体はユーザ情報記憶部１１３に記憶された正当な情報である。本実施形態ではユーザＩＤやパスワードを不正に入手した場合であっても、ＩＰアドレスを用いて正当なセッション設定要求であるか否かを判定できるようになっている。

【００２４】［２．実施形態の動作］次に、本実施形態の動作として、図４～図６に示すフローチャートを参照しながらセキュリティゲートウェイの動作を説明した後に、図７～図９に示すシーケンスを参照しなが全体の具体的動作を説明する。

【００２５】［２－１．セキュリティゲートウェイの動作］

［２－１－１．セッション設定要求時の動作］図４は、セキュリティゲートウェイ１１０のセッション設定要求時における動作を示すフローチャートである。セキュリティゲートウェイ１１０は、セッション設定要求を受けると（Ｓ１）、まず当該セッション要求についての認証を行う（Ｓ２）。ここでは、認証制御部１１２は、先に説明したユーザ情報記憶部１１３およびアクセス拒否情報記憶部１１４に記憶された情報（図３参照）に基づいては正当なユーザからの要求か否かを判定する。ステップＳ２の認証において、正当なユーザからのセッション設定要求ではないと判定した場合は（Ｓ２；ＮＧ）、ステップＳ１において受けたセッション設定要求を拒絶する（Ｓ３）。

【００２６】一方、ステップＳ２の認証において、正当なユーザからのセッション設定要求であると判定した場合は（Ｓ２；ＯＫ）、次に、同時接続セッション数のチェックを行う（Ｓ４）。同時接続セッション数のチェックとは、同一のユーザＩＤを有するクライアントが同時にセッション設定を行うことを制限するための処理である。具体的には、セッション要求を行ったクライアントが示すユーザＩＤと同一のユーザＩＤに対応したセッション情報が当該チェック時においてセッション情報記憶部１１６に記憶されている場合には、同時接続セッション数をこえていると判定する。ステップＳ４において、同時接続セッション数をこえていないと判定した場合は（Ｓ４；ＯＫ）、当該セッション設定要求に対するセッション設定処理を行う（Ｓ５）。セッション設定処理は、サーバ側セキュリティゲートウェイ１１０のセッション資源の枯渇を解消するための処理であり、より詳しくは、図５および図７を参照しながら後に説明する。一方、ステップＳ４において、同時接続セッション数をこえていると判定した場合は（Ｓ４；ＮＧ）、不正接続防止処理を行う（Ｓ６）。不正接続防止処理は、すでにセッション情報が記憶されているユーザＩＤと同一のユーザＩＤを示すセッション設定要求が、正当なユーザからのものであるか否かを判定する処理であり、より詳しくは、図６～図９を参照しながら後に説明する。

【００２７】［２－１－２．セッション設定処理］次に、図５に示すフローチャートを参照しながら、セッション設定処理（図４：Ｓ５）について説明する。セッション設定処理では、セキュリティゲートウェイ１１０はまず総セッション数制限チェックを行う（Ｓ５１）。セッション情報記憶部１１６に記憶することが可能な総セッション数には予め制限が設けられており、この制限を

こえてセッション設定要求があった場合にはサーバ側のセッション資源が枯渇する。そこで、セッション制御部１１５は、セッション設定要求時においてセッション情報記憶部１１６に記憶されているセッション数が当該制限の範囲内であるか否かを判定する。

【００２８】ステップＳ５１のチェックにおいて、セッション数が当該制限の範囲内であると判定した場合は（Ｓ５１；ＯＫ）、セッション制御部１１５は、セッション設定要求に対するセッション設定を行う（Ｓ５２）。一方、ステップＳ５１のチェックにおいて、セッション数が当該制限の範囲内ではないと判定した場合は（Ｓ５１；ＮＧ）、セッション制御部１１５は、セッション情報記憶部１１６に記憶されているセッション情報の中から、削除すべき候補セッションを選択する（Ｓ５３）。記憶されているセッション情報の中には、上述したような「死んでいるセッション」が含まれいる可能性があり、このような「死んでいるセッション」を削除することによってセッション資源の枯渇を解消することができる。

【００２９】本実施形態では、次に説明する２種類のアルゴリズムのいずれかを用いて、削除してよい可能性の高いセッションを選択する。

①ＦＩＦＯ（First In First Out）

最も古く作成されたセッションを削除するアルゴリズムである。このアルゴリズムを用いて削除セッションの候補を選択する場合には、例えば、セッション制御部１１５は、セッションを作成した順番にセッション番号が付されるようにセッション情報を生成し、セッション情報記憶部１１６に記憶されているセッション情報の中から最も小さなセッション番号を有するものを、削除セッション候補として選択する。このような場合は、新規にセッション情報を生成する際に、その時点で最も大きなセッション番号が付されるようにすればよい。

②ＬＲＵ（Last Recently Used）

最も古く使用されたセッションを削除するアルゴリズムである。このアルゴリズムを用いて削除セッションの候補を選択する場合には、例えば、セッション制御部１１５は、セッションを使用した順番にセッション番号が付されるようにセッション情報を生成し、セッション情報記憶部１１６に記憶されているセッション情報の中から最も小さなセッション番号を有するものを、削除セッション候補として選択する。この場合は、通信が行われる毎にその時点で最も大きなセッション番号が再度付されようにすればよい。

【００３０】ステップＳ５３において削除候補セッションの選択を行うと、セッション制御部１１５は、選択された削除候補セッションに対応するクライアントに対して状況確認メッセージを送信し（Ｓ５４）、当該クライアントから正常な応答があったか否かを判定する（Ｓ５５）。ここでは、所定期間内にクライアントから応答がない場合や、予め規定された応答とは異なる応答あるいは何らかの異常を示す応答（異常応答）があった場合に、クライアントからの応答がないと判定される。ステップＳ５５の判定において、クライアントからの応答があったと判定した場合は（Ｓ５５；あり）、ステップＳ５３において選択されたセッションを削除候補の最後に置き換え（Ｓ５６）、ステップＳ５３に移行して再度削除候補セッション選択を行う。例えば、最も小さなセッション番号の付されたセッション情報を削除候補として選択している場合であれば、当該セッション情報中のセッション番号をその時点で最も大きなセッション番号に更新することによって、削除候補の最後に置き換える。一方、ステップＳ５５の判定において、クライアントからの応答がなかったと判定した場合は（Ｓ５５；なし）、ステップＳ５３において選択した当該セッションを削除して、セッション要求に対するセッションを設定する（Ｓ５７）。

【００３１】［２－１－３．不正接続防止処理］次に、図６に示すフローチャートを参照しながら、不正接続防止処理（図４：Ｓ６）について説明する。不正接続防止処理では、セキュリティゲートウェイ１１０は旧セッションのＩＰアドレスに対して状況確認メッセージを送信し（Ｓ６１）、当該状況確認メッセージに対する応答が有るか否かを判定する（Ｓ６２）。セッション制御部１１５は、セッション情報記憶部１１６に記憶されているセッション情報から、セッション設定要求を行っているクライアントのユーザＩＤと同一のユーザＩＤに対応して記憶されているＩＰアドレスを旧セッションのＩＰアドレスとして抽出し、当該ＩＰアドレスを宛先とした状況確認メッセージパケットを送信する。なお、状況確認メッセージには、同一のユーザＩＤを示すセッション設定要求があった旨を警告するメッセージが含まれている。

【００３２】ステップＳ６２の判定において、状況確認メッセージに対する応答がなかった場合は（Ｓ６２；なし）、セッション制御部１１５は、状況確認を行ったＩＰアドレスが割り当てられた移動端末４００とパケットゲートウェイ３６０（インターネット接続点）との接続が切断され、当該ＩＰアドレスに対応した旧セッションが死んでしまったと判定し、旧セッションを削除してセッション設定要求に対して新セッションを設定する（Ｓ６３）。より具体的には、状況確認を行ったＩＰアドレスに対応したセッションが死んでいる場合に、同一ユーザＩＤを示す新たなセッション要求がある場合とは、何らかの理由で移動端末４００とパケットゲートウェイ３６０との接続が切断された後に、再度接続し直したために通信端末４００に対して新たなＩＰアドレスが割り当てられた可能性が高い。そこで、セッション制御部１１５は、このような場合にはセッション接続要求は正当なユーザからのものであると判定する。また、同時セッシ

ョン数制限を解消するために旧セッションをセッション情報記憶部から削除する。これに対して、ステップＳ６２の判定において、状況確認メッセージに対する応答があった場合は（Ｓ６２；あり）、状況確認を行ったＩＰアドレスに対応したセッションは生きている、すなわち、当該ＩＰアドレスの割り当てられた移動端末４００と企業ＬＡＮ１００は接続された状態にあるにもかかわらず、第三者が不正に接続しようとしていると判定し、セッション設定を拒絶する（Ｓ６４）。

【００３３】［２－２．実施形態の具体的動作］

［２－２－１．総セッション数制限をこえた場合］まず、図７を参照しながら、総セッション数制限が２であるセキュリティゲートウェイ１１０に対して、３以上の移動端末４００がそれぞれセッション設定要求を行うことによって、総セッション数制限の範囲をこえた場合の動作について説明する。図７においては、図１に示す移動端末４１１がユーザＩＤ“Client1”として、移動端末４１２がユーザＩＤ“Client2”として、移動端末４１３がユーザＩＤ“Client3”として、それぞれセッション設定要求を行う。なお、図７においては、各移動端末４００似対して割り当てられたＩＰアドレスに関する情報は省略している。

【００３４】移動端末４１１がユーザＩＤ“Client1”としてセキュリティゲートウェイ１１０へのセッション設定要求を行う（Ｓ１０１）。このとき、セッション制御部１１５は、セッション情報記憶部１１６に記憶されているセッション情報を参照して総セッション数制限の範囲内であると判定し、新たにセッション情報を生成する。この新たなセッション情報には、この時点で最も大きなセッション番号＃１が付される。新たなセッション情報を生成するとセキュリティゲートウェイ１１０は、移動端末４１１に対してセッション設定の応答を行い（Ｓ１０２）、移動端末４１１と企業ＬＡＮ１００との仮想私設網２１０を介した通信を行うことができるようになる。

【００３５】次に、移動端末４１２がユーザＩＤ“Client2”としてセキュリティゲートウェイ１１０へのセッション設定要求を行う（Ｓ１０３）。このとき、セッション制御部１１５は、セッション情報記憶部１１６に記憶されているセッション情報を参照して総セッション数制限の範囲内であると判定し、新たにセッション情報を生成する。この新たなセッション情報には、この時点で最も大きなセッション番号＃２が付される。新たなセッション情報を生成するとセキュリティゲートウェイ１１０は、移動端末４１２に対してセッション設定の応答を行い（Ｓ１０４）、移動端末４１２と企業ＬＡＮ１００との仮想私設網２１０を介した通信を行うことができるようになる。

【００３６】セキュリティゲートウェイ１１０における総セッション数制限は２であるから、この時点でセッション資源が枯渇しており、その後に移動端末４１３がユーザＩＤ“Client3”としてセキュリティゲートウェイ１１０へのセッション設定要求を行うと（Ｓ１０５）、セッション制御部１１５は、セッション情報記憶部１１６に記憶されているセッション情報を参照して総セッション数制限の範囲をこえたと判定する。そこで、セッション制御部１１５は、この時点で最も小さなセッション番号＃１の付されたセッション情報を「死んでいる」可能性の高い削除候補セッションとして選択し、セッション番号＃１に対応して記憶されているユーザＩＤ“Client1”を示す移動端末４１１に対して状況確認メッセージを送信する（Ｓ１０６）。移動端末４１１が状況確認メッセージに対して正常な応答を行うと（Ｓ１０７）、セッション制御部１１５は、選択されたセッション情報のセッション番号＃１をこの時点で最も大きなセッション番号＃３に更新する。セッション番号＃１がセッション番号＃３に更新されることによって、“Client1”に対応するセッション情報は削除候補の最後に置き換えられ、この時点で最も小さなセッション番号は＃２となる。

【００３７】ところで、移動端末４１２は、セッション設定後に圏外へ移動しており（Ｓ１０８）、パケットゲートウェイ３６０との接続が切断されている。従って、セッション番号＃２の付されたセッションは「死んだ」状態になっている。しかしながら、セキュリティゲートウェイ１１０においては、移動端末４１２とパケットゲートウェイ３６０との接続が切断されていることは検出していないので、セッション制御部１１５はセッション番号＃２の付されたセッション情報を削除候補として選択し、セッション番号＃２に対応して記憶されているユーザＩＤ“Client2”を示す移動端末４１２に対して状況確認メッセージを送信する（Ｓ１０９）。移動端末４１２とパケットゲートウェイ３６０との接続が切断されているので、この状況確認メッセージは移動端末４１２に到達せず、セキュリティゲートウェイ１１０に対しては何ら応答がなされない、あるいは異常な応答がなされることになる（Ｓ１１０）。セッション制御部１１５はセッション番号＃２の付されたセッションは「死んでいる」と判定してセッション情報を削除し、移動端末４１３がユーザＩＤ“Client3”として行ったセッション設定要求に対するセッション情報を生成する。この新たなセッション情報には、この時点で最も大きなセッション番号＃４が付される。新たなセッション情報を生成するとセキュリティゲートウェイ１１０は、移動端末４１３に対してセッション設定の応答を行い（Ｓ１１１）、移動端末４１３と企業ＬＡＮ１００との仮想私設網２１０を介した通信を行うことができるようになる。

【００３８】このように、セキュリティゲートウェイ１１０は、総セッション数制限の範囲をこえた時点で「死んでいる」可能性の高い削除候補セッションを選択し、順次セッションが生きているか否かの状況確認を行い、

「死んでいる」セッションと確認できたセッションを削除していくので、削除ミスの可能性を極めて小さくすることができる。また、キープアライブパケットを使用しなくても「死んでいる」セッションを削除できるので、キープアライブパケットに対する課金がなくなり、移動端末４００のユーザは通信コストを削減することができる。

【００３９】［２－２－２．同一ユーザが再度セッション設定要求した場合］次に、図８を参照しながら、移動端末４１１がセッション設定後にいったんパケットゲートウェイ３６０との接続を切断し、再接続後にセッション設定要求を行うことによって、同一ユーザが再度セッション設定要求した場合の動作について説明する。図８に示す例においては、移動端末４１１が最初にパケットゲートウェイ３６０に接続したときに割り当てられるＩＰアドレスは“123.456.78.9”であり、切断後に再接続したときに割り当てられるＩＰアドレスは“223.456.78.9”である。

【００４０】移動端末４１１のユーザインターフェイスからユーザＩＤおよびパスワードが入力されると（Ｓ２０１）、移動端末４１１は、ユーザＩＤ“Client1”としてセキュリティゲートウェイ１１０へのセッション設定要求を行う（Ｓ２０２）。このとき、セッション制御部１１５は、セッション情報記憶部１１６に記憶されているセッション情報を参照して同時接続セッション数の範囲内であると判定し、新たにセッション情報を生成する。この新たなセッション情報には、この時点で最も大きなセッション番号＃１が付される。新たなセッション情報を生成するとセキュリティゲートウェイ１１０は、移動端末４１１に対してセッション設定の応答を行い（Ｓ２０３）、移動端末４１１と企業ＬＡＮ１００との仮想私設網２１０を介した通信を行うことができるようになる。

【００４１】その後移動端末４１１とパケットゲートウェイ３６０との接続が切断されると、セッション番号＃１の付されたセッションは「死んだ」状態となるがセキュリティゲートウェイ１１０は移動端末４１２とパケットゲートウェイ３６０との接続が切断されている状態は検出しないので、セッション番号＃１の付されたセッション情報はそのままセッション情報記憶部１１６に保存される。そして、移動端末４１１がパケットゲートウェイ３６０に再接続し、ＩＰアドレス“223.456.78.9”が割り当てられる（Ｓ２０５）。ここで、移動端末４１１のユーザインターフェイスからユーザＩＤおよびパスワードが入力されると（Ｓ２０６）、移動端末４１１は、ユーザＩＤ“Client1”としてセキュリティゲートウェイ１１０へのセッション設定要求を行う（Ｓ２０７）。このとき、セッション制御部１１５は、セッション情報記憶部１１６に記憶されているセッション情報を参照して同時接続セッション制限数をオーバーしたことを検出し、当該セッション情報に対応したＩＰアドレス“123.456.78.9”を宛先とした状況確認メッセージを送信する（Ｓ２０８）。

【００４２】移動端末４１１とパケットゲートウェイ３６０との接続が切断されたときに移動端末４１１に対するＩＰアドレス“123.456.78.9”の割り当ては解放されているので、ＩＰアドレス“123.456.78.9”を宛先とした状況確認メッセージに対する応答は行われない（Ｓ２０９）。そこで、セッション制御部１１５は、状況確認を行ったセッション情報を削除し、ステップＳ２０７におけるセッション設定要求に対する新たなセッション情報（図中セッション番号＃ｎ）を生成する。新たなセッション情報を生成するとセキュリティゲートウェイ１１０は、移動端末４１１に対してセッション設定の応答を行い（Ｓ２１０）、移動端末４１１と企業ＬＡＮ１００との仮想私設網２１０を介した通信は、ＩＰアドレス“123.456.78.9”から“223.456.78.9”に引き継がれて、継続して行うことが可能となる。

【００４３】このように、移動端末４１１がセッション設定後にいったんパケットゲートウェイ３６０との接続を切断し、再接続後にセッション設定要求を行うような場合には、セッション資源の枯渇を待たずに「死んでいる」セッションを早期に削除することができるので、セッション状態をより正確に管理することができるようになる。

【００４４】［２－２－３．不正接続を防止する場合］次に、図９を参照しながら、移動端末４１１がユーザＩＤ“Client1”としてセッション設定後、ハッカーが移動端末４２０からユーザＩＤ“Client1”としてセッション設定要求した場合の動作について説明する。図９に示す例においては、移動端末４１１がパケットゲートウェイ３６０に接続したときに割り当てられるＩＰアドレスは“123.456.78.9”であり、移動端末４１１がパケットゲートウェイ３６０に接続したときに割り当てられるＩＰアドレスは“987.654.32.1”である。

【００４５】移動端末４１１のユーザインターフェイスからユーザＩＤおよびパスワードが入力されると（Ｓ３０１）、移動端末４１１は、ユーザＩＤ“Client1”としてセキュリティゲートウェイ１１０へのセッション設定要求を行う（Ｓ３０２）。このとき、セッション制御部１１５は、セッション情報記憶部１１６に記憶されているセッション情報を参照して同時接続セッション数の範囲内であると判定し、新たにセッション情報を生成する。この新たなセッション情報には、この時点で最も大きなセッション番号＃１が付される。新たなセッション情報を生成するとセキュリティゲートウェイ１１０は、移動端末４１１に対してセッション設定の応答を行い（Ｓ３０３）、移動端末４１１と企業ＬＡＮ１００との仮想私設網２１０を介した通信を行うことができるようになる。

【００４６】次に、ハッカーが不正に入手したユーザＩＤ“Client1”およびパスワードを用いて、移動端末４２０からユーザＩＤ“Client1”としてセキュリティゲートウェイ１１０へのセッション設定要求を行う（Ｓ３０４）。このとき、セッション制御部１１５は、セッション情報記憶部１１６に記憶されているセッション情報を参照して同時接続セッション制限数をオーバーしたことを検出し、当該セッション情報に対応したＩＰアドレス“123.456.78.9”を宛先とした状況確認メッセージを送信する（Ｓ３０５）。このメッセージはＩＰアドレス“123.456.78.9”が割り当てられたままになっている移動端末４１１に到達するので、移動端末４１１は、状況確認メッセージに対する正常な応答を行う（Ｓ３０６）とともに、ユーザインターフェイスに警告メッセージを表示させる（Ｓ３０７）。応答を受けたセキュリティゲートウェイ１１０は、ステップＳ３０４でうけたセッション設定要求を拒絶して（Ｓ３０８）、拒絶したセッション設定要求が示すユーザＩＤ“Client1”とＩＰアドレス987.654.32.1”とを対応つけてアクセス拒否情報として登録する。

【００４７】その後、移動端末４２０から再度セッション設定要求があった場合には（Ｓ３０９）、セキュリティゲートウェイ１１０はアクセス拒否情報を参照することによって、ユーザＩＤ“Client1”を示すセッション設定要求であっても、ＩＰアドレス987.654.32.1”であればハッカーからの要求であると判定してセッション設定を拒絶することができる（Ｓ３１０）。また、移動端末４１１のユーザは、ユーザインターフェイスに表示される警告メッセージなどによりハッカーの存在を認識し、パスワードの変更などの対処を行う。

【００４８】このように、悪意の第三者（ハッカー）が正当なユーザの認証情報を不正に入手してセッション設定要求を行う場合には、すでに記憶されているセッション情報の中から同一の認証情報を有するＩＰアドレスに対して状況確認メッセージを送信することによって、ハッカーによる不正な接続を防止できるようになる。

【００４９】［３．変形例］本発明は、上述した実施形態に限定されるものではなく、以下のような各種の変形が可能である。

【００５０】上記実施形態においては、クライアント側の端末装置を移動端末４００を例として説明したが、インターネット接続点と通信網を介して接続可能であればどのようなものでもよい。同様に、上記実施形態では、サーバ側のネットワークを企業ＬＡＮ１００を例として説明したが、インターネットとの接続が可能であればどのようなものでもよく、行政サービス用のネットワークや家庭内のインターネット対応機器で構成したネットワークなどでもかまわない。また、通信網もＰＤＣパケット通信網３００に限らず、送受信データ量に対して課金されるものであれば他の通信網であってもよい。インターネット接続点についても、パケットゲートウェイ３６０に限らず他のプロバイダであってもよいのはもちろんである。

【００５１】上記実施形態では、セッション設定要求に含まれる認証情報として、ユーザＩＤおよびパスワードを例として説明したが、これに限らず、デジタル署名など他の情報であってもよい。また、アドレス情報についても、ＩＰアドレスに限らず、クライアントの端末と特定する他の情報であってもよい。

【００５２】上記実施形態では、削除候補セッション情報を選択するための所定の規則としては、ＦＩＦＯあるいはＬＲＵすなわち、選択される優先順位は生成されてからの経過時間が長いあるいは最後に使用されてからの経過時間が長いセッション情報である程高いものを例として説明しているが、これに限らず、セッションが「死んでいる」可能性が高いものを選択できれば他の規則であってもかまわない。また、生成されてからの経過時間が長いあるいは最後に使用されてからの経過時間を示す情報として、上記実施形態ではセッション番号を用いて説明しているが、これに限らず、時刻そのものをセッション情報に含ませるようにしてもよいし、他のパラメータを用いてもかまわない。

【００５３】

【発明の効果】以上説明したように、本発明によれば、クライアントとサーバとを接続する仮想私設網において、安定的な通信を確保しながら低コストでセッション情報の資源枯渇を防止するが可能となる。

【図面の簡単な説明】

【図１】　実施形態の全体構成を示す図である。

【図２】　セキュリティゲートウェイの構成を示す図である。

【図３】　記憶する各種情報を説明する図である。

【図４】　セキュリティゲートウェイの動作を説明するフローチャートである。

【図５】　セッション設定処理を説明するフローチャートである。

【図６】　不正アクセス防止処理を説明するフローチャートである。

【図７】　総セッション数制限をこえた場合の具体的動作を説明するシーケンスである。

【図８】　同一ユーザが再度セッション設定要求した場合の具体的動作を説明するシーケンスである。

【図９】　不正接続を防止する場合の具体的動作を説明するシーケンスである。

【符号の説明】

１００…企業ＬＡＮ、
１１０…セキュリティゲートウェイ、
２００…インターネット、
２１０…仮想私設網
３００…移動通信網、

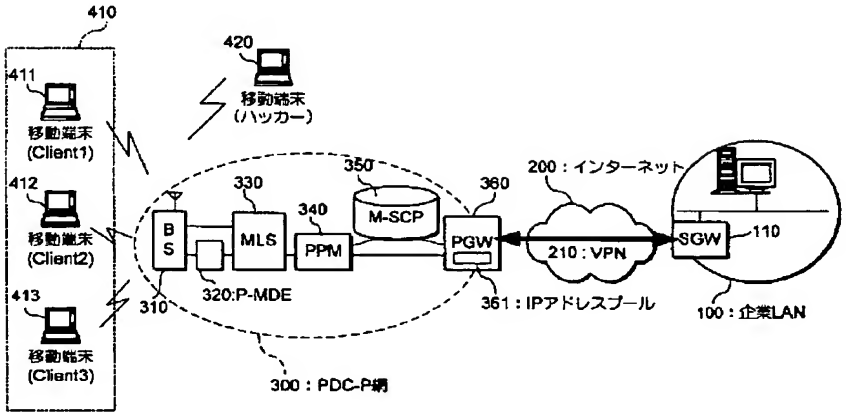
21

３１０…基地局、
３２０…パケット用基地局変復調装置、
３３０…加入者交換機、
３４０…パケット加入者系処理装置、

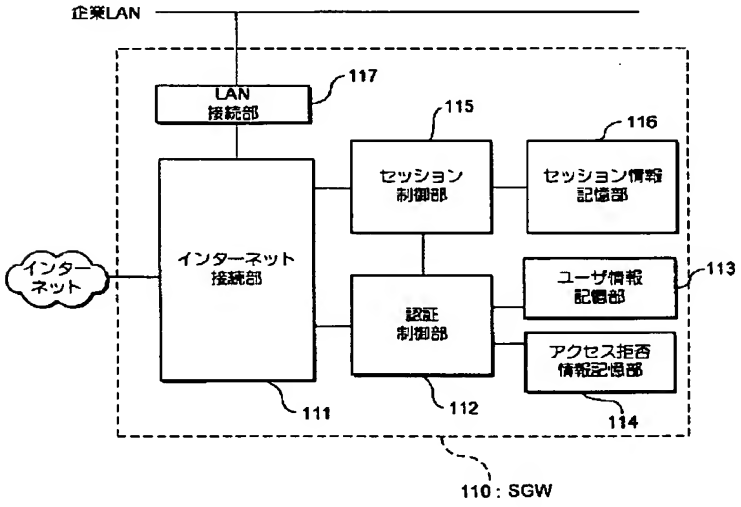
22

＊３５０…移動通信サービス制御装置、
３６０…パケットゲートウェイ、
３６１…ＩＰアドレスプール、
＊　４１１、４１２、４１３、４２０…移動端末。

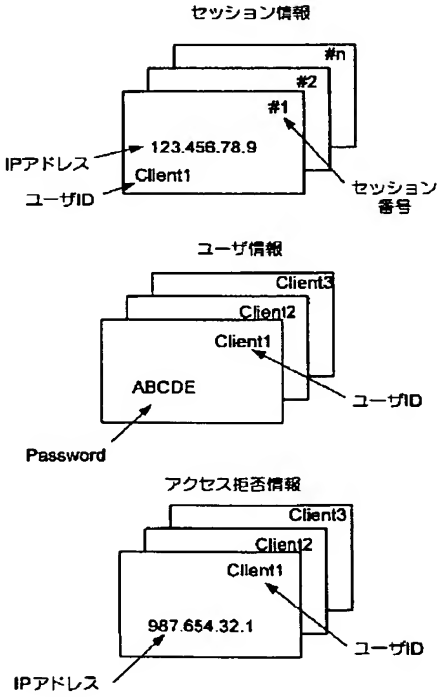
【図１】



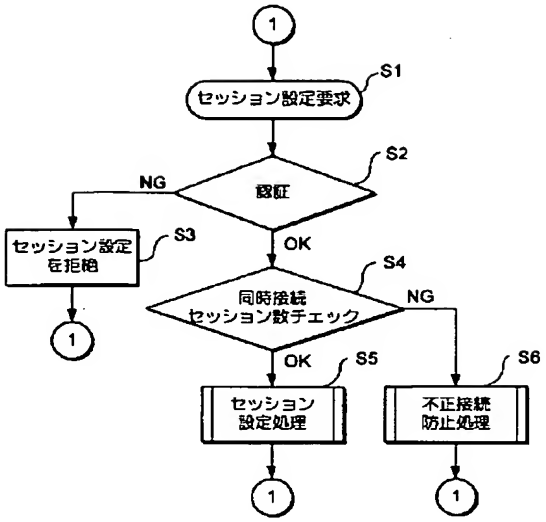
【図２】



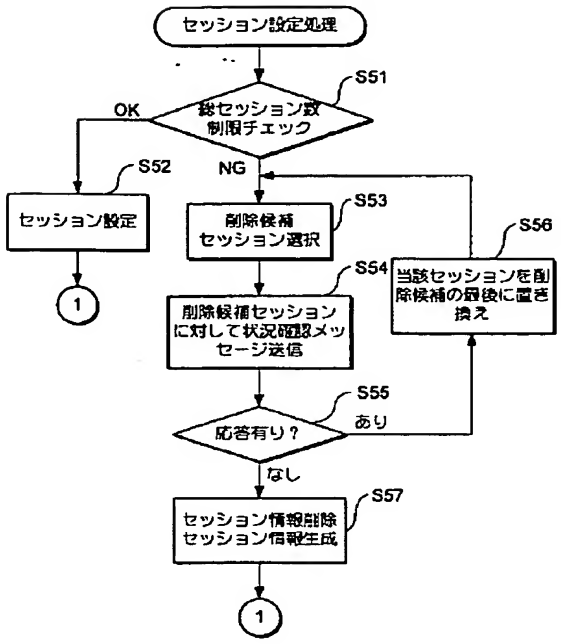
【図３】



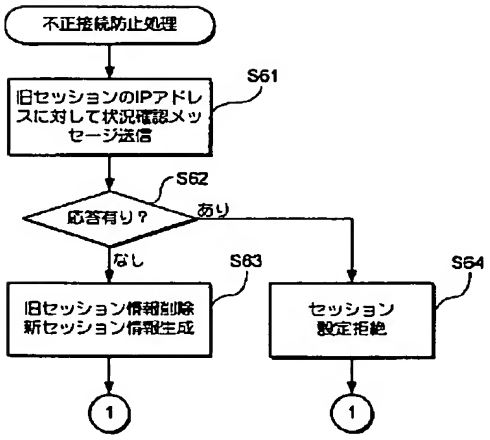
【図４】


1
セッション設定要求
S1
認証
S2
NG
OK
セッション設定を拒絶
S3
同時接続セッション数チェック
S4
NG
OK
セッション設定処理
S5
不正接続防止処理
S6
1
1
1

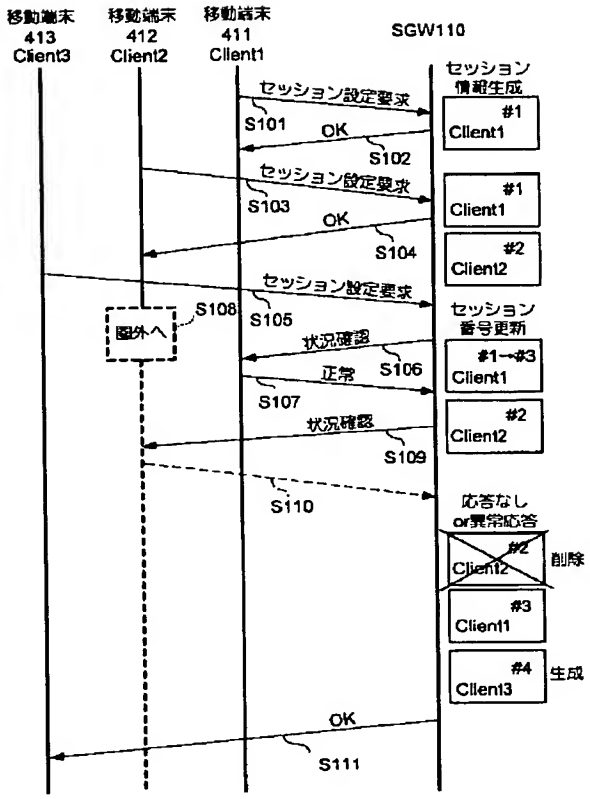
【図５】


セッション設定処理
総セッション数制限チェック
S51
OK
NG
セッション設定
S52
削除候補セッション選択
S53
当該セッションを削除候補の最後に置き換え
S56
削除候補セッションに対して状況確認メッセージ送信
S54
応答有り？
S55
あり
なし
セッション情報削除セッション情報生成
S57
1
1

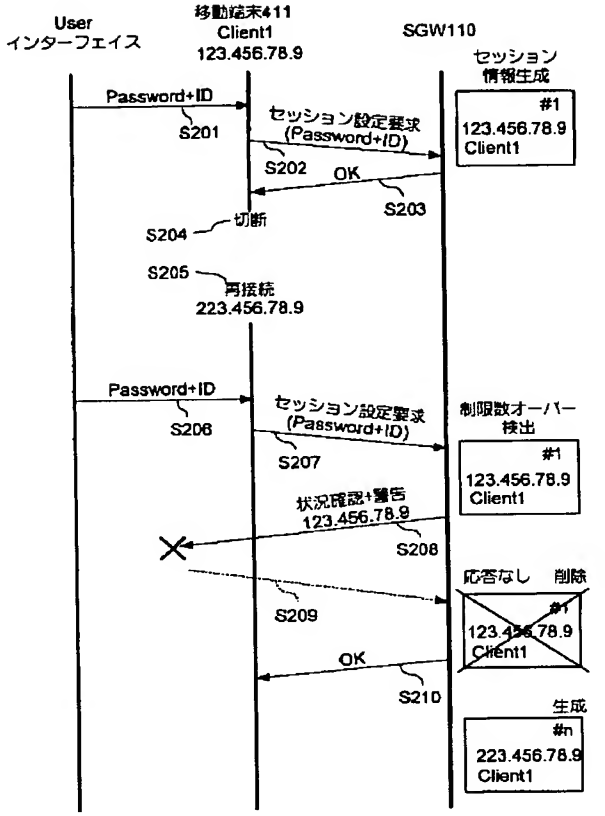
【図６】


不正接続防止処理
旧セッションのIPアドレスに対して状況確認メッセージ送信
S61
応答有り？
S62
あり
なし
旧セッション情報削除新セッション情報生成
S63
セッション設定拒絶
S64
1
1

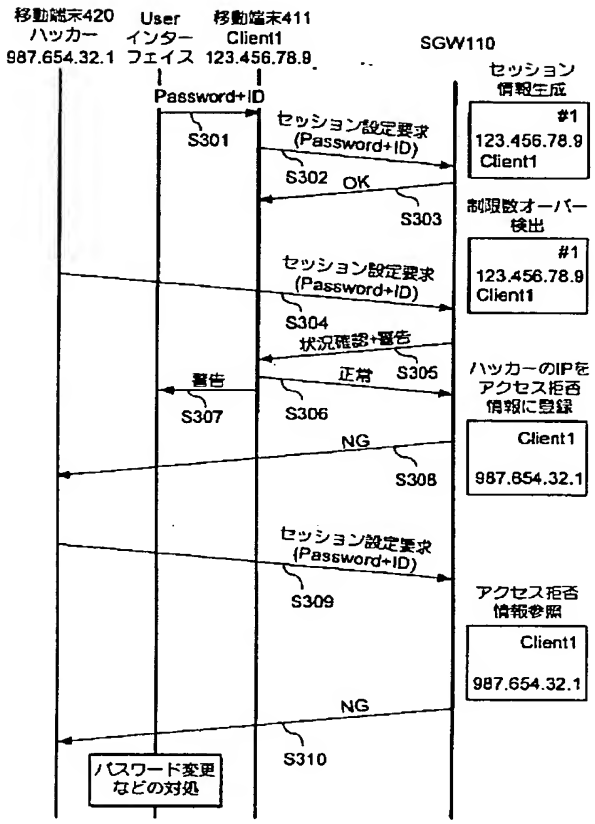
【図７】


移動端末
413
Client3
移動端末
412
Client2
移動端末
411
Client1
SGW110
セッション
情報生成
セッション設定要求
S101
OK
S102
セッション設定要求
S103
OK
S104
セッション設定要求
S105
圏外へ
S108
セッション
番号更新
状況確認
正常
S106
S107
状況確認
S109
S110
応答なし
or異常応答
削除
生成
OK
S111
#1
Client1
#2
Client2
#1→#3
Client1
#2
Client2
#3
Client1
#4
Client3

【図８】


User
インターフェイス
移動端末411
Client1
123.456.78.9
SGW110
セッション
情報生成
Password+ID
S201
セッション設定要求
(Password+ID)
S202
OK
S203
S204
切断
S205
再接続
223.456.78.9
Password+ID
S206
セッション設定要求
(Password+ID)
S207
制限数オーバー
検出
状況確認+警告
123.456.78.9
S208
S209
応答なし
削除
OK
S210
生成
#1
123.456.78.9
Client1
#n
223.456.78.9
Client1

【図９】



フロントページの続き

(72)発明者　関口　克己
東京都港区虎ノ門二丁目10番１号　エヌ・
ティ・ティ移動通信網株式会社内

Ｆターム(参考)　5B089 GA31 HA01 KA12 KA16 KB06
KB11 KC28 KC39 KC51 KC54
KC58 KG01 KG03 MA02 MC01
5K030 GA15 HA08 KA04 KA05 LA03
LB02 LC18 LD20